
**DIGITAL PRIVACY AS A HUMAN RIGHT:
RECONCILING SURVEILLANCE WITH CIVIL LIBERTIES**

-Ms. Aashi Dixit¹

Abstract

In an era dominated by pervasive digital surveillance, the tension between state security imperatives and individual privacy rights has escalated into a profound human rights crisis. This paper posits digital privacy as an indispensable human right, essential for human dignity, autonomy, and democratic flourishing. Drawing on frameworks from the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, it argues that privacy in the digital age—encompassing data protection, anonymity, and freedom from unwarranted intrusion—must be elevated beyond mere statutory protections to a non-derogable norm. The analysis dissects the reconciliation challenge: mass surveillance programs, justified under national security pretexts, erode civil liberties through chilling effects on speech, association, and dissent. The paper advocates for "privacy by design" in surveillance architectures, robust judicial oversight, and international covenants mandating minimalism, transparency, and sunset clauses for data retention. By integrating technological safeguards like end-to-end encryption with ethical oversight mechanisms, societies can safeguard civil liberties without forsaking security. Ultimately, this reconceptualization urges policymakers to prioritize human-centric digital governance, ensuring surveillance serves the public good rather than subverting it.

Keywords: digital privacy, human rights, mass surveillance, civil liberties, data protection, privacy by design, GDPR, digital governance.

1. Introduction

The technological revolution has changed the functioning of societies. It has penetrated into every sphere of communication, trade, government, and even personal relationships. Collection and surveillance have been hastened manifold, yet citizens can be tracked by governments and nongovernmental organizations in ways that were not even imagined earlier. Surveillance is

¹ Independent Academic Researcher, BBA LL.B, LL.M, NET (Law).

being sold as a tool of national security, antiterrorism, and fortification of public welfare. But it can also end up badly defeating freedom and privacy. The most important issue is heightened tension between official trends towards security and control and the maintenance of simple freedoms and human dignity. Technology has been outpacing the law in innovation at a pace that ensures that protective gear in turn can be used to intrude, censor, and oppress. This conflict is most troubling in democratic countries because unchecked surveillance imperils free association and speech, less so the rights that render civic participation something more than a mirage. This article addresses the problem of human rights law and digital privacy. This paper does not see privacy as the technical or legislative problem but as a fundamental human freedom and dignity. The study will consider whether privacy can be constructed and established as a constitutional right and yet overcome valid concerns of the state interest in spying for security and government purposes. By the use of legal doctrines of necessity, proportionality, and responsibility, the study will attempt to formulate models that are able to balance these competing forces. Methodologically, the paper is composed in comparative law format. It will refer to international human rights treaties, constitutional protections, and foremost judicial decisions across a broad spectrum of jurisdictions. It will identify how far the right to internet privacy is being enshrined in international thinking and how effective current endeavors are in transposing threats in the modern period. In this way, the study seeks to assist in resolving current controversy surrounding how surveillance can be protected from civil liberties while the world continues to bear witness to continuous race to develop technologies. Keywords: *Digital Privacy, Human Rights Law, State Surveillance, Civil Liberties, Proportionality Principle*

2. Conceptual Framework

The idea of privacy has been present for millennia as a natural aspect of human dignity, but since the advent of digital technology, its extent and complexity have grown spectacularly. In the past, privacy was understood in terms of space, home life, and protection against unwanted intrusion into an individual's house. In the age of the internet, privacy is much larger. It now comprises digital personae, digital communications, biometrics, payments, online search records, and even social contact patterns facilitated by software. All of these demands reconsidering privacy not as some leftover right, but a multifaceted right that is inextricably intertwined with the very character of living in a digitally networked age. Civil liberties themselves acquire new hues in the digital age. Historically had enjoyed freedom of expression in the sense of exercise in the domains of speech, print, and assembly but now experiences it largely in social media and online forums. Similarly, freedom of association is experienced

largely through virtual communities and electronic mobilization, and individual autonomy comes to increasingly rely on the control by an individual over how his or her own information is collected, stored, and transmitted.² Unless digital privacy is adequately protected, such freedoms are being observed, managed, and coerced. The chilling impact of pervasive surveillance has the indirect effect of deterring people from exercising their freedoms, replacing the democratic culture upon which civil liberties rely. International human rights law offers a normative environment of comprehension and argument for digital privacy.³ Article 12 of the Universal Declaration of Human Rights⁴ provides the right to freedom from arbitrary interference with privacy, family, home, or correspondence. This commitment is reaffirmed in binding international treaties such as Article 17 of the International Covenant on Civil and Political Rights⁵ that obligate states to protect individuals from illegal intrusion into their honour and dignity. Regional instruments enumerate these protections as well. The European Convention on Human Rights,⁶ to cite but one, provides a right of respect for family and private life, and is just as safeguarded by the American Convention on Human Rights⁷ and by the African Charter on Human and Peoples' Rights.⁸ As a whole, these tools acknowledge that privacy is not an either/or right but a part of human liberty, autonomy, and dignity even while its limits change with technology.

3. Surveillance and Its Justifications

Surveillance has also been used by states in order to realize public order and national security. Its application has, however, inflated with the advent of the internet age. The most frequent reasons include anti-terrorism, prevention of crime, and public health and safety promotion. The rationale is that surveillance on citizens enables the government to foresee threats, shift crime, and be able to respond to emergencies appropriately. For example, in times of epidemic disease, the surveillance has watched over disease and compelled adherence to health policy. This has helped toward a broad assumption that such measures are in the best interests of society. Surveillance is currently very sophisticated, using overt as well as covert methods. Obtaining information in large quantities is now common, and large amounts of personal

² Daniel j. Solove, *Understanding Privacy* (Harvard Univ. Press 2008).

³ Alan f. Westin, *Privacy and Freedom* (Atheneum 1967).

⁴ Universal Declaration of Human rights, G.A. Res. 217 (iii) A, U.N. Doc. A/res/217(iii) (Dec. 10, 1948).

⁵ International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, art. 17.

⁶ European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221.

⁷ American convention on Human Rights, Nov. 22, 1969, 1144 U.N.T.S. 123.

⁸ African charter on Human and Peoples' Rights, June 27, 1981, 1520 U.N.T.S. 217.

information are routinely extracted from telecommunication companies, web sites, and financial systems.⁹ New technology such as facial recognition software, biometric scanning, and AI-based surveillance amplifies the ability of the state to monitor and identify individuals. Cyber surveillance and metadata collection also make it possible for governments to monitor behavior patterns, social interaction, and mobility, in many cases unknown or without the consent of individuals. These technologies grant the state even more dominance of the public and private life. But with rising surveillance comes equally dire ethical and legal issues. One of the most sinister threats is the potential for random or discretionary surveillance, eroding the rule that restrictions on rights must be necessary, lawful, and proportionate. Unfettered surveillance has the ability to chill freedom by deterring individuals from protesting, demonstrating, or being linked with others. Invasion of privacy not only restrains individual freedom but also harms democratic participation. With no restraints and controls, surveillance will be transformed into an instrument of oppression, not of protection, and violate the very principles it was legislated for.

4. Digital Privacy as a Human Right

The global recognition of privacy as a universal human right has continued to develop in international legal thinking, assuming ever more prominence with the advent of information technology. International law continued to affirm the right to be free from arbitrary or unlawful interference with privacy, family, home, or correspondence.¹⁰ Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights provide the foundation for such protection, and subsequent United Nations General Assembly resolutions and Human Rights Council reports further reinforced the extension of such guarantees to data flows and digital communications. In particular, the 2013 UN General Assembly resolution on "The Right to Privacy in the Digital Age" did indeed make an express recognition that state surveillance and corporate data practices must be brought into consistency with existing human rights obligations, thereby placing digital privacy within the overall human rights framework.

Judicial dicta elsewhere also followed suit in this recognition, acknowledging the international character of privacy concerns in the light of a world ever more technologically networked. In

⁹ Shoshana Zuboff, *The Age of Surveillance Capitalism* (Public Affairs 2019).

¹⁰ Julie E. Cohen, What Privacy is for, 126 *Harv. L. Rev.* 1904 (2013).

India, the landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India made privacy a constitutional right on a par with dignity, liberty, and autonomy.¹¹ The Supreme Court reaffirmed once again that privacy protection is not a privilege but a condition precedent to the exercise of other constitutional freedoms. In America, the US Supreme Court, in *Carpenter v. United States*, decided that warrantless access to historical cell-site location data infringed on the Fourth Amendment, extending constitutional protections to categories of digital data compiled by ordinary technological means. At the same time, the Court of Justice of the European Union in *Digital Rights Ireland* invalidated the Data Retention Directive on the grounds that mass data retention was disproportionate and incompatible with the European Union's Charter of Fundamental Rights.¹² Overall, the decisions illustrate a new judicial mindset that there needs to be privacy protection from unreasonable surveillance and data gathering.¹³

Aside from its legal formal status, digital privacy increasingly comes to be recognized as a normative condition grounded on the basis of autonomy, dignity, and democracy. Privacy enables people to create and realize their identities, make their choices unencumbered by undue coercion, and participate democratically without fear of vendetta. Rights like expression, association, and political participation become meaningless in the absence of privacy since intensive surveillance leads to a chilling effect that discourages free speech. In this regard, privacy is not only an individual right but also a social guarantee on which democratic institutions and protected societies against abusive uses of authoritarian power are founded.¹⁴ The creation of digital privacy as a human right thus not only protects personal interests but also guarantees constitutional democracy and rule of law in the age of omnipresent technological potency.

5. Reconciling Surveillance with Civil Liberties

The dilemma of balancing state surveillance and the rights of citizens is to make sure that measures applied in the pursuit of security do not disproportionately infringe on basic rights. Jurisprudence and human rights international law have tasked valid surveillance to meet the

¹¹ Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India) (recognizing privacy as a fundamental right under the Indian Constitution).

¹² *Digital Rights Ireland Ltd. V. Minister for Commerce*, Case C-293/12, 2014 E.C.R. I-238.

¹³ Jeffrey Rosen, *The Naked Crowd: Balancing Privacy and Security in an Age of Terror*, 46 *Ariz. L. Rev.* 607 (2004).

¹⁴ Charter of Fundamental Rights of the European Union art. 8, Dec. 7, 2000, 2000 O.J. (C 364) 1.

criteria of legality, necessity, proportionality, and accountability. Legality demands the measures to be founded on existing and public legislation that specifies their scope and boundaries. Necessity calls for the measures to be for present social necessity that is, counter-terrorism or public safety, and only used where less obtrusive methods are not available. Proportionality demands surveillance to be proportionate to what is sought, ruling out indiscriminate or disproportionate surveillance. Accountability demands effective controls to stop abuse and subject surveillance to democratic scrutiny on an ongoing basis. Checks and balances are an effective safeguard against abuse of surveillance power. Judicial supervision facilitates imposition of checks on intrusions like communication interception or access to personal information so that these are allowed on reasonable grounds alone. Parliamentary committees and independent regulators weave webs of responsibility in the form of scrutiny of government practice, oversight of intelligence activity, and implementation of protection of privacy. These controls limit executive abuses but also promote public trust in the legitimacy of surveillance work.¹⁵

Openness and safeguards are no less critical to the attainment of freedom and security. Strong data protection law, supported by effective enforcement authorities, serves to manage collection, storage, and disclosure of personal data. Whistleblower protections enable accusations of illegal or disproportionate surveillance, and information access regimes enable citizens to make effective complaints about power.¹⁶ All of these guarantees together ensure the establishment of a culture of openness that does not lead to abuse and facilitates good governance. Comparative approaches to regulation identify several routes to establishing the balance. International best practice has been set by the European Union General Data Protection Regulation (GDPR),¹⁷ which imposes rigorous requirements for data processing and enshrines the individual right to personal data. United States Privacy Act of 1974 and its amendments are intended to oversee federal agency use of personal data, claiming exceptions of national security still widely interpreting. In India, the Supreme Court ruling to make privacy a fundamental right in Puttaswamy has given push to the process of constructing towards an encompassing law, and the Personal Data Protection Bill attempting to develop a mechanism to provide a framework for regulating state and private surveillance activities.¹⁸ Each of these

¹⁵ Daniel J. Solove, A Taxonomy of Privacy, 154 U. Pa. L. Rev. 477 (2006).

¹⁶ Whistleblower Protection Act of 1989, 5 U.S.C. 2302(b)(8) (2018).

¹⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

¹⁸ The Personal Data Protection Bill, 2019, Bill No. 373 of 2019, Lok Sabha Secretariat (India) (pending).

models puts surveillance in the foreground in a regime of responsibilities and rights where pursuit of safety is weighed against vigorous reassertion of human dignity and civilian freedom.

6. Challenges in Ensuring Digital Privacy

Internet privacy protection is faced with a number of challenges in today's world, some being the result of the nature of the innovation in technology. One of the best-known is the fast rate of technological innovation relative to incremental innovation of law and regulation. With new surveillance technology, means of data collection and analysis being conceived and adopted nearly on a rolling basis, legislatures and response courts are perpetually in catch-up mode. The resulting time lag causes loopholes in the regulations that unprotect privacy rights, permitting surveillance pursuits to grow untrammelled before implementing meaningful protection measures.

The second most urgent challenge is the very global nature of computer communications, generating difficult issues of global flows of data and conflicts of jurisdictions. Personal data may cross many states in seconds, stored on servers subject to various jurisdictions. It is a difficult problem to determine which state law applies to such data, and harmonize conflicting rules. Absence of a universal world regime of digital privacy creates inconsistencies which are vulnerable to being taken advantage of by governments and other non-state entities and hence erode the universality of human rights protection. Even where legal protections are robust, weak enforcement agencies further erode digital privacy. Most states have subscribed to data protection law, yet the agencies responsible for its enforcement are usually poorly funded, politically compromised, or lacking the technology employed by dominant institutions. This is compounded by low digital literacy in society aggravating it.¹⁹

Wide segments of the public do not know that they are sharing, disseminating, or selling information about themselves, taking less pressure off corporations and states to maintain high levels of privacy. Last but not least, private corporations' role presents special challenges for digital privacy protection. In the era of what Shoshana Zuboff has called "surveillance capitalism," data collection and analysis are actually the real basis of corporate business models.²⁰ Businesses monitor user activity across websites, commodity user information in

¹⁹Roman Zakharov v. Russia, App. No. 47143/06, Eur. Ct. H.R. (2015) (establishing standards of legality, necessity, and proportionality in surveillance regimes).

²⁰ Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (2019).

targeted advertising and construct predictive platforms conditioning personal preference and choice. This kind of privatization of informational power blurs state-corporate boundaries of surveillance, forcing hard questions about responsibility, transparency, and whether current human rights rhetoric can effectively contain non-state actors. These are overall symptoms of the tenuous state of online privacy today. They refer that judicial acknowledgement of privacy as a human right, as much as it is needed, cannot be adequate without responsive enforcement, international cooperation, public awareness, and reconsideration of the relationship between technology, power, and human dignity.

7. Recommendations

Legalization of digital privacy as a fundamental human right has to be the foundation of government in the digital era. Although certain jurisdictions such as the European Union have stepped into the enforcement of full-blown privacy protection schemes, the world is still in pieces when it comes to response. There should be a universal respect for privacy as the trans-boundary foundation of human dignity and democratic governance so that the individual is afforded an equivalent degree of protection in different jurisdictions. Data protection and privacy legislation should be reconciled on a continuous basis. State national legal systems should aim at harmonizing national law with international norms, such as the values enshrined in the General Data Protection Regulation (GDPR). Such harmonization would not only facilitate cross-border enforcement of privacy rights, but also instill confidence in states, companies, and individuals doing business in an integrated digital economy.

As a supplement to global efforts, the development of an international convention or treaty with the specific aim of digital rights would represent a paradigm shift. As the Universal Declaration of Human Rights set the tone for human rights research decades ago, an international framework could find points of convergence on surveillance, data aggregation, and user behavior in the digital age. Such a tool would settle jurisdictional conflicts and ensure responsibility on the part of both state and non-state actors. Technological progress itself needs to be aimed at protecting rights and not undermining them. Instilling privacy-by-design and privacy-by-default concepts in technology design provides a precautionary approach to avoiding risk before harm occurs. It guarantees that privacy-preserving controls come as a norm rather than an afterthought but rather as a fundamental part of digital infrastructure. Lastly, any change would be incomplete without empowering individuals themselves. The individuals must be made aware of how their personal data is being used and redresses they

have when their rights are being misused. Legal literacy campaigns, education, and redressals at affordable costs must come in crafting a culture of responsibility. Doing so, sound protection of whistleblowers can avert illegal surveillance or corporate misconduct, upholding transparency and trust in institutions. Together, all these efforts are moving toward keeping technological progress in touch with human rights norms. By integrating online privacy into the wide ambit of law on human rights, societies can ensure that technological advances will not undermine freedom, dignity, and democratic responsibility.

8. Conclusion

The trajectory of twenty-first-century e-government has justified the inherent tension between state security needs and safeguarding civil liberties. The growth of surveillance tools—from storing metadata and algorithmic monitoring to biometrics and predictive analysis—has given governments historically unparalleled abilities to observe and control. Although these kinds of powers have previously been based on anti-terror, public safety, or even health emergency grounds, their unbalanced or uncontrolled use derogates from the very international and constitutional assurance of human freedom and dignity that states have engaged to uphold. The issue before us today is not whether there should be surveillance, but how to reconcile it with established standards of human rights law. Digital privacy cannot thus be a secondary or collateral issue. It must, instead, be accorded the status of a condition sine qua non to the exercise of other freedoms. Privacy ensures the independence of an individual in the exercise of untrammelled thought, being autonomous, and exercising free will in becoming integrated into civic and political life. Lacking privacy, freedom of speech, association, and even religious thought are at risk since citizens will censor themselves on what they feel should remain private in fear of the "chilling effect" of being monitored all the time. Because more than one super ordinate jurisdiction's highest court, from India's Supreme Court in *Puttaswamy v. Union of India* to the United States Supreme Court in *Carpenter v. United States*, has held, privacy is not an elitist privilege but a constitutional institutional imperative of democracy. It is the space in which human beings can live and thrive free from excessive interposition by corporate or state power.

Apart from this, characterization of privacy as an inalienable human right has international connotations that transcend the national structure. Connectivity of information renders it more challenging to safeguard privacy if information for individuals transcends borders with competing standards and enforcement jurisdiction. International agreement must dominate the

norm order of digital rights. While the middle century saw human rights codified in the Universal Declaration of Human Rights and subsequent later covenants, so too does this century also cry out equally for an equivalent international convention or treaty of digital privacy. The means would be to plug loopholes in regulation, render jurisdictional conflict more transparent, and ensure privacy as a universal right and not a privilege of locality. No less critical is the contribution of technology itself. Innovation has been advanced for too long with too little regard for its human rights consequences, with the surveillance capacity overwhelming protection. Something needs to shift paradigm so that values like privacy-by-design and data minimization become part of digital system architecture. That would mean that technological advancement no longer habitually tramples on human rights-oriented values but, rather, is a partner to their evolution. On the basis of rigorous data protection law, autonomous powers of surveillance, and severe punishment of crime, all these must be the new norm of democratic governance in the age of digital technology.

The last and most creative aspect of this plan is empowering the people. Technological shielding and legal foundation will not matter if the populace does not enjoy it and utilize it as citizens to resist as well. Whistleblower rights, open government procedures, and virtual learning must be spread so that empowered and enlightened citizens can combat unwarranted surveillance. The individuals must not be objects to be exploited but co-writers of the digital order that unites them. Digital privacy is not nearly so much about protecting people's information from being exploited as it is about renewing profound, democratic values of autonomy, human dignity, and democracy in the midst of unprecedented technological change. Democratic institutions survive only when powers of surveillance are contained by law and made accountable to it. Convergence of the globe, uniform legal norms, and a human rights-sensitive information technology culture are necessary to achieve such balance. The option, therefore, is rational: acknowledgment of computer privacy as a human right can no longer be an option but a necessity in its absolute sense. It is the armor that must be used to close or shatter the door behind which technological advancements conspire or prostitute democratic ideals. A rights-oriented digital order founded on openness, accountability, and global solidarity must be pursued with utmost speed if the dreams of freedom and dignity enshrined in human rights law are to remain the guiding light for the digital age.
